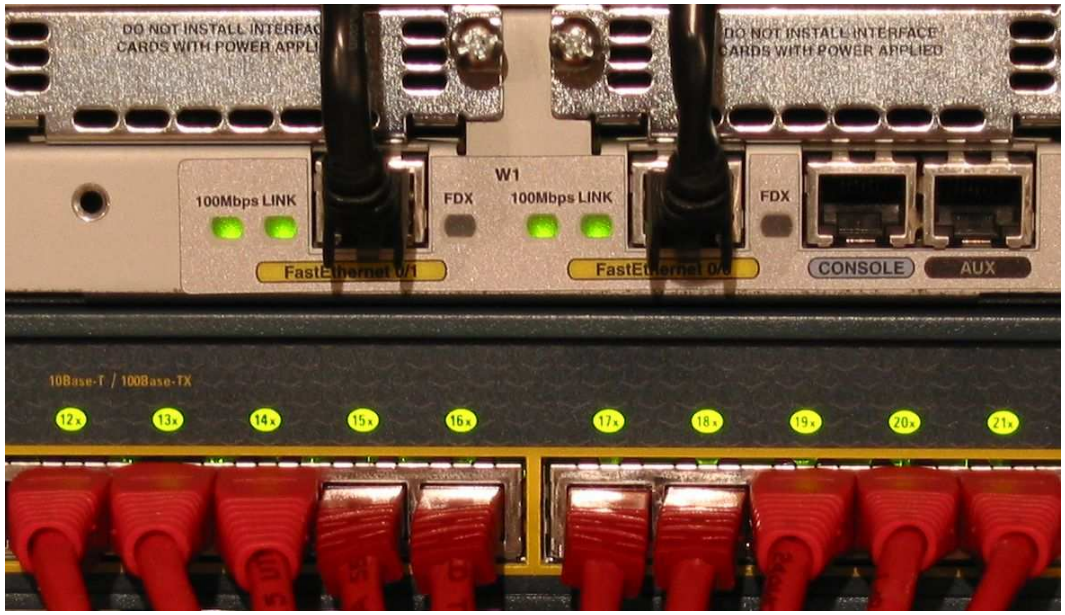
CIRT-Level Response to Advanced Persistent Threat

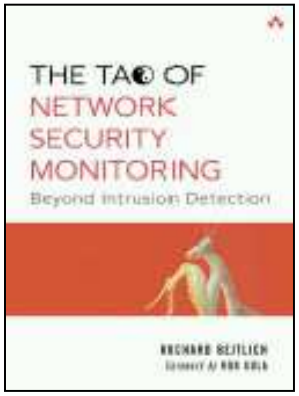


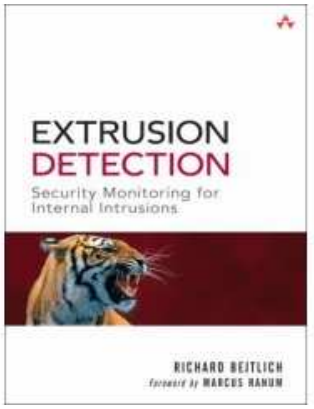
TAOSECURITY
THE WAY OF DIGITAL SECURITY

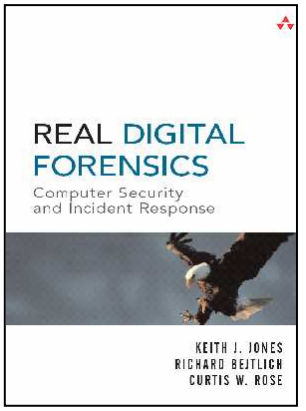
Richard Bejtlich
Director of Incident Response, General Electric
richard@taosecurity.com
taosecurity.blogspot.com

Introduction

- Bejtlich ("bate-lik") biography
  - General Electric, (07-present)
  - TaoSecurity (05-07)
  - ManTech (04-05)
  - Foundstone (02-04)
  - Ball Aerospace (01-02)
  - Captain at US Air Force CERT (98-01)
  - Lt at Air Intelligence Agency (97-98)
- Author
  - Tao of Network Security Monitoring: Beyond Intrusion Detection (solo, Addison-Wesley, Jul 04)
  - Extrusion Detection: Security Monitoring for Internal Intrusions (solo, Addison-Wesley, Nov 05)
  - Real Digital Forensics (co-author, Addison-Wesley, Sep 05)
  - Contributed to Incident Response, 2nd Ed and Hacking Exposed, 4th Ed
  - TaoSecurity Blog (http://taosecurity.blogspot.com)







Assumptions

- You are an APT victim.
- You care.
- You have hope.

Remember Red, hope is a good thing, maybe the best of things, and no good thing ever dies...

I hope I can make it across the border. I hope to see my friend and shake his hand. I hope the Pacific is as blue as it has been in my dreams.

I hope.

- Andy, The Shawshank Redemption

Critical Themes

- Prevention eventually fails.
- Persistent threats never give up.
- Winning does not mean preventing compromise. Rather:
  - Increase $/MB

  - Predict next move

  - Track adversary change

  - Intrusion suppression

terremark

Favorite Kris Harms APT Quotes (FIRST 2010)

- “Compliance is the floor upon which you’re going to fall when you get hacked.”
- “Today a B [grade] is not good enough.”
- “Do not get in a battle over knowledge of Windows with an intruder. You will lose.”
- “Lesley Stahl, I pwn your wireless.”

http://www.cbsnews.com/video/watch/?id=3538299n

First Hour after D-Zero

- Document everything.
- Change communication patterns.
- Activate your IR plan.

D-Zero + 1 hour

First Day after D-Zero

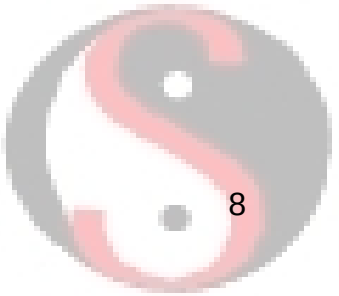
- Switch to alternative computing platforms.
- Implement trustworthy communication.
- Inventory security data.

D-Zero + 1 day

First Week after D-Zero

- Decide to enlist external help.
- Deliver initial briefing to decision makers.
- Analyze available security evidence.
- Begin deploying additional instrumentation.

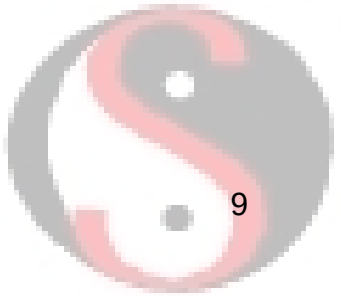
D-Zero + 1 week



First Month after D-Zero

- Determine incident scope.
- Evaluate effectiveness of security instrumentation.
- Plan remediation.

D-Zero + 1 month



First Year after D-Zero

- Evaluate IR capability effectiveness
- Institutionalize counter-APT ops.
- Develop and embed counter-APT improvements.
- Collaborate with peers.
- Expand security instrumentation.
- Hire help.

D-Zero + 1 year

Second Year after D-Zero

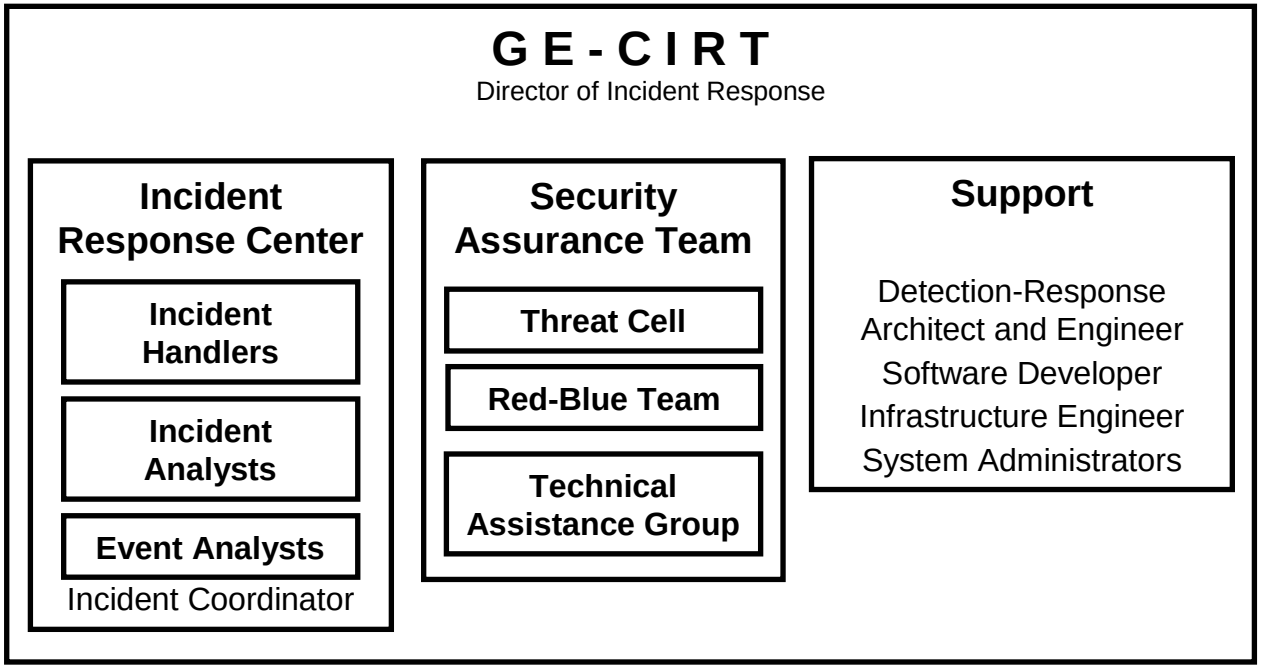
- Create Red-Blue Team.
- Develop security intelligence capability.
- Contribute to industry counter-APT work.
- Continue hiring help.

D-Zero + 2 years

Containment vs Honeynet?

- Reasons to *not* immediately contain/disconnect victims *when you are new to counter-APT* ops:
  - Scope of incident likely unknown.
  - Disconnecting victims removes intelligence source.
  - Adversary will notice and change tools, tactics, and procedures.
- When to start disconnecting? *When you meet your win criteria.*

Suggested CIRT Structure



Hiring Priorities

- Incident Handlers - subject matter experts who will establish early credibility and competency
- Event Analysts - 24x7 coverage to support more routine work
- Incident Analysts - assume the natural balance between IH and EA work
- Support team - transfer design, build, and run activities from the IRC to Support
- Threat cell - profile adversaries and professionalize reporting
- Blue team - provide collaborative assessment assistance
- Technical Assistance Group - internal security consulting
- Incident Coordinator - quality control for IRC operations
- Red team - adversary replication and simulation

Peer incident detection and response teams

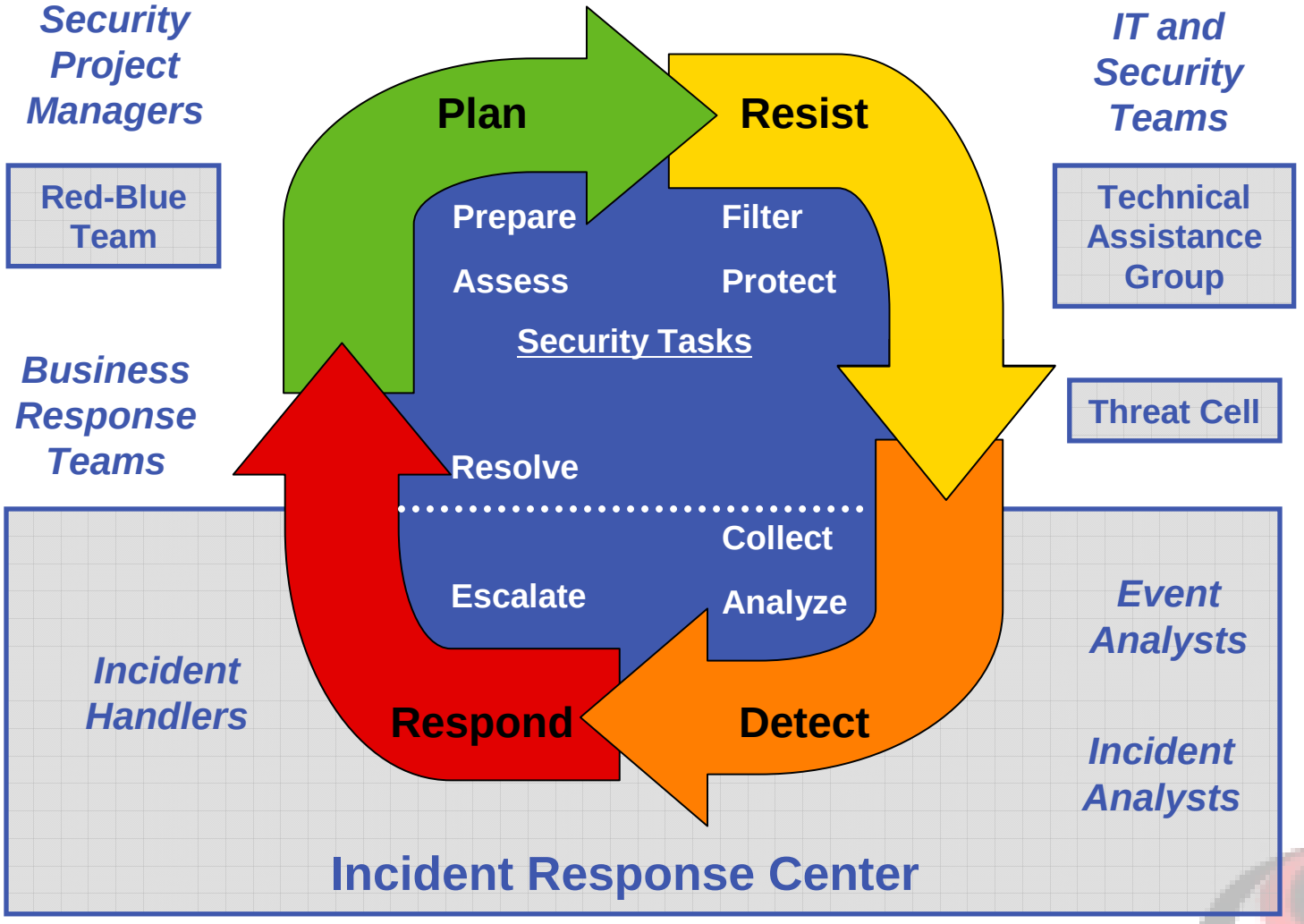
Company	Team Name	Employees	Team FTE	Contractors	FTE per EC	FTE + Contractor per EC	CIRT FTE per 10,000 employees
General Electric	GE-CIRT	296,000	12	3	.000041	.000051	0.41
Aerospace 1 [1]	IRT	XXX,000	11	0	.000073	.000073	0.73
Aerospace 2 [1]	NOSC / SecEng	XX,000	13	0	.000289	.000289	2.89
DIB 1 [1]	Sec Ops	XXX,000	11	1	.000088	.000096	0.88
DIB 2 [1]	CSIRT	XX,000	5	2	.000076	.000106	0.76
DIB 3 [1]	DIB3-CIRT	XXX,000	50	0	.000345	.000345	3.44
DIB 4 [1]	DIB4CERT	XX,000	42	2	.000575	.000603	5.75
Aerospace 3 [1]	IRT	X,000	2	0	.000500	.000500	5
Silicon Valley 1 [3]	CIRT	XX,000	24	0	.000366	.000366	3.66
Software Company 1 [3]	IRT	XX,000	41	0	.000442	.000442	4.42
Software Company 2 [2]	Sec Ops Center	X,000	15	0	.001875	.001875	18.75
Utility Company 1 [2]	Sec Ops Center	XX,000	16	0	.000800	.000800	8

5 IR per 10,000 employees

- Average FTE per EC (AFPE): .000456
- Average FTE + Contractor per EC (AFCPE): .000462
- Implied GE-CIRT FTE for GE based on AFPE: 134 FTEs
- Implied GE-CIRT FTE for GE based on AFCPE: 136 FTEs + Contractors

Sources
- 2009 DSIE survey [1]
- 2008 EIMP project [2]
- 2009 EIMP project [3]

Incident Cycle



Note: GE-CIRT Components

Questions?

KNOW YOUR NETWORK BEFORE AN INTRUDER DOES

```
40.652146 10.145.15.100 -> 216.68.1.200 DNS Standard query A z3n.phatcamp.org
40.690278  10.142.1.89 -> 216.68.1.100 DNS Standard query A z3n.phatcamp.org
40.690291  10.142.1.89 -> 216.68.1.100 DNS Standard query A z3n.phatcamp.org
41.386313 10.145.15.98 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
43.386117 10.145.15.100 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
43.386248 10.145.15.100 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
44.568156  10.142.1.97 -> 10.145.15.100 DNS Standard query A z3n.phatcamp.org
46.258206  10.142.1.89 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
46.258210  10.142.1.89 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
46.258292  10.142.1.89 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
46.258306  10.142.1.89 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
48.062938  10.142.1.97 -> 10.142.1.89  DNS Standard query A z3n.phatcamp.org
```

Richard Bejtlich

richard@taosecurity.com

taosecurity.blogspot.com